ABSTRACT

In one aspect of the invention, embodiments of the invention can superimposed upon the existing framework of network which includes a number of nodes interconnected by the underlying communications network. In one embodiment, an access control node is interposed between each node and the remainder of the network. The access control node is adapted to transmit information about the node and the user attempting to access the node to a server used for maintaining security and audit information. This information may take the form of node identification data (thus identifying the node) and user identification data (to ensure that the user is associated with an active account and the user has entered the correct password thus authenticating the user). If the node is not recognised by the server, then no access to protected information (e.g., PHI) is allowed. If, however, the node is recognised, then access to PHI requires that the user also be authenticated. Assuming both conditions exist, aspects of the invention will determine (based on a repository of information about users) the data each user is entitled to access and the functionality of the node that is to be made available to the user. Aspects of the invention may place limitations on the functionality offered by the node to which the user should be granted access. That is, although a user may be attempting to access data from a node which has a set of functions (e.g., printing, storing data to a removable media, displaying video signals, etc.), aspects of the invention enable only a subset of these functions to be made available depending on the rights which have been granted to a user.